IN THE CLAIMS

The claims as they currently stand are as follows:

Claims 1-13 (Cancelled)

14. (Currently Amended) A method for personalizing GSM chips, wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki comprising the steps of:

a) performing the personalization of the chip when the subscriber logs on to the subscriber network for the first time;

b) obtaining the (ICCID) card number and the (IMSI) subscriber identification number from a number pool, the chip itself derives an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip, while PIN and PUK are set to a default value;

c) making an entry in an authentication center (AC) and a home location register (HLR) as soon as the subscriber has entered into a contract with a network operator;

d) deriving at the authentication center (AC) the initial secret key Ki_1;

e) setting the conditions of the network so that during logon to the network, a connection is established from the chip to the security center (SC) of the network operator;

f) routing the connection from the chip to the security center (SC) during the first logon;

g) negotiating between the chip and the security center (SC) a new second secret key Ki_2 for the chip;

h) unconditionally disabling the conditions of step e).

15. (Previously Presented) The method according to claim 14, wherein the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the authentication center (AC) before the contract is established.

16. (Previously Presented) The method according to claim 14, further comprising the step of employing a Diffie-Hellman method to negotiate the second secret key Ki_2.

17. (Previously Presented) The method according to claim 16, wherein the home location register (HLR) is capable of setting and deleting a rerouting command (hotlining flag).

18. (Previously Presented) The method according to claim 17, wherein, when the initial secret key Ki_1 is entered into the authentication center (AC) for the first time, the hotlining flag is also set in the home location register (HLR).

19. (Currently Amended) A chip having a memory, wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki are stored, wherein the chip itself derives an initial secret key Ki_1 and, wherein the chip in the terminal equipment is Toolkit-enabled and includes means for communicating with a security center (SC) and negotiating a new secret key Ki_2 for the chip.

20. (Previously Presented) The chip according to claim 19, wherein the chip includes means for receiving data from the security center (SC) and means for writing the received data to the memory.

21. (Previously Presented) The chip according to claim 20, wherein the chip comprises a microprocessor for negotiating a secret key with the security center (SC).

22. (Previously Presented) The chip according to claim 21, wherein the chip includes a dialing number which is fixedly programmed by the manufacturer.

23. (Previously Presented) The method according to claim 14, wherein PIN and PUK default values are stored at the chip.

24. (Previously Presented) The method according to claim 14, wherein step g) further comprises negotiating at the security center (SC) the PUK with the chip or generated in the security center (SC) and transmitted to the chip.

25. (Previously Presented) The chip according to claim 19, wherein PIN and PUK default values are stored at the chip.

26. (Previously Presented) The chip according to claim 19, wherein the chip includes means for reading data received from the security center (SC) in memory, modifying the data and transmitting the data to the security center (SC).